EXHIBIT 2

Case 1:04-cr-10217-GAO Document 75-3 Filed 03/03/2006 Page 2 of 7

Guidance merges incident response with forensics

By Sam Stover, Network World, 10/17/05

CLEAR CHOICE TEST Guidance Software's most recent release of EnCase Enterprise puts incident-response capabilities into the IT security manager's toolbox. In our Clear Choice Test, we found that with this aggregation of incident-response and forensic capabilities not yet seen in competing products, EnCase Enterprise can (for a pretty big price tag) help a network investigator establish relationships between open ports, open files, network connections, hidden files or processes and malicious network activity.

Tapping IDS for automated incient response
Archive of Network World tests
Subscribe to the Network Product Test Results newsletter

Unix and Linux administrators are always going to have tools/utilities such as lsof (list open files), netstat (list open ports and more), bvi (binary file editing) and a bevy of other (even more capable) incident-response tools. However, that approach is limited in a corporate environment by the effort required to coordinate these disparate tools.

Advertisement:

Imagine that your

Network World's HOT SEAT with John Gallant
Five minutes. Unscripted. Unexpected

A better way to virtualiz
In this week's Network Wor seat, CEO John Thibault ma bold case for why Virtual Ir data center virtualization b than the big boys. Watch it

All Hot Seat videos

Today's 10 most-read stories

1. World's largest Windows error message
2. Teenager claims to find code flaw in Gmail
3. Forum: Strange user requests
4. Forum: Application acceleration across the WA
5. Microsoft's Origami Project is...
6. CCIE: Talk about a stress test
7. Wacky requests from end users
8. Seven products for your next-gen data center
9. See Microsoft's Origami right now
10. GENI: A sneak peek at what's after the Intern

Check out the latest security threat map brought to you by Trend Micro

Security
VENDOR SOLUTIONS
Want to Simplify Identity

NEWSLETTERS
Sign up for one c NWW's Network Security newslet
- Security in P
- Virus and Bu Alert
- Security

Case 1:04-cr-10217-GAO Document 75-3 Filed 03/03/2006 Page 3 of 7

Webcasts
Partner Sites
-Data Explosion
-Ent. Infrastructure
-ProCurve Networking
-Enterprise Server
-Perimeter Security
-Evolving Data Center
-Web Security
-Storage Ecosystem

SITE RESOURCES

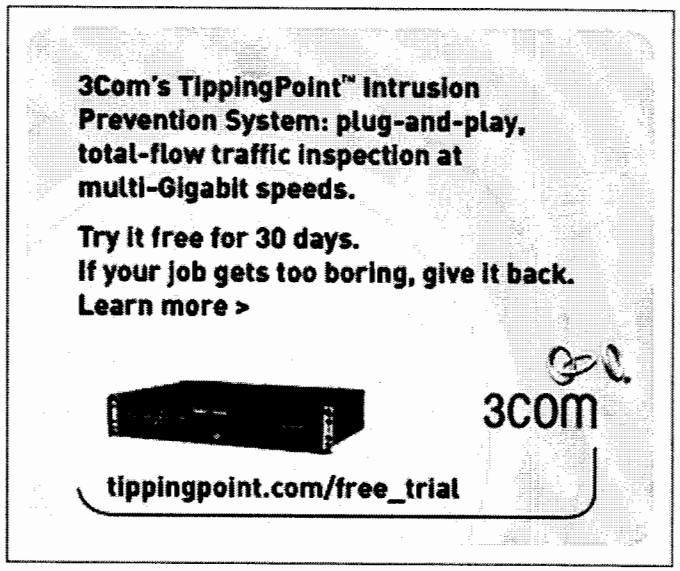
Product Tests
Buyer's Guides
Video Library
Threat Map
Demo.com
Careers NEW
Newsletters
This Week in Print
Opinions
Blogs
Encyclopedia
Forums
RSS Feeds
Special Issues
Network Life

ABOUT US

NW SUBSCRIPTION

Special Issues

Signature Series



network intrusion-detection system (IDS) generates an alert that shows traffic to Port 2222 on your Web server. Then, seconds later, your host-based IDS for that same machine generates an alert showing that the kernel has been modified. Then you have to access the box via a Secure Shell (SSH) connection (or traipse to the building where the box physically sits to use the console) and start nosing around to see what is going on.

With EnCase Enterprise, you receive the IDS alerts, swivel your chair to a different console and pull that same information - all transparent to the potential attacker who could be watching for a root logon via local or SSH connection. While there is a bit of a learning curve to complete some complex forensic investigation, getting started with basic functions such as checking for open ports, running processes and suspicious files (plus any relationship between them) is rather easy.

There are three parts to the EnCase Enterprise system: the Secure Authentication for EnCase (SAFE), the Enterprise Examiner GUI front end and the Servlet agent software.

SAFE takes care of all authentication processes. Each user is assigned a profile in the SAFE that defines what resources he can access.

The Examiner GUI - EnCase Enterprise's bread and butter from a security analysis point of view - bears a striking resemblance to the interface of the more law enforcement- focused EnCase Forensic edition. Overall, the GUI lets you navigate easily between the parameters you've established and the detailed file or port and process information you'll need to investigate.

Management?
- Quest Software

E-Policy Best Practices Guide
- St. Bernard

"The Definitive Guide to Active Directory Disaster Recovery"
- NetPro Computing Inc

Virtual Media: Optimizing Operations Efficiency
- Avocent

Network World Special Report: Securing Wireless Enterprises, Today's Management Challenge , click here to download
- Siemens

More...

TOP 10 WORLDWIDE THREATS

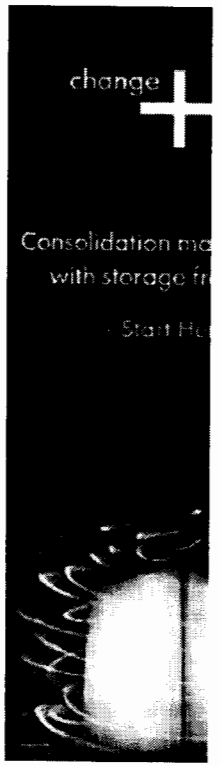
TREND MICRO

WORM NYXEM.E
SPYW DASHBAR.300
SPYW GATOR.F
JAVA BYTEVER.A
HTML NETSKY.P
JAVA BYTEVER.A-1
WORM NETSKY.P
JAVA FEMAD.B
TROJ DMSEC.A
WORM BAGLE.CL

Security Nev
VPNs
Messaging
View all newsletters

Email Address:

Sponsored Link
Free Tech Day S
Learn from Syma
Experts how to P
Your Network. Er
Today!



Case 1:04-cr-10217-GAO Document 75-3 Filed 03/03/2006 Page 4 of 7

Best Products Issue NEW

Enterprise All-Star NEW 2006 nominations now open

New Data Center

Next-generation IT NEW

Lastly, Servlet agents run on monitored boxes and communicate with the Examiner. This agent works at a basic level in the operating system and allows the analyst access to detailed information about the host. The Servlet is completely reactive; ir presents information to the Examiner only when queried. It has almost no effect on the host's performance, unless an investigator is taking action.

A primary tenet of incident response built into EnCase Enterprise is the ability to remove from consideration, as fast as possible, the "known good," be it ports, files, processes, log entries or even registry entries. The faster an analyst can filter through what is known and focus on what is unknown, the shorter the investigation time. In some enterprise environments, IDS alerts can easily number in the tens of thousands each day. In most cases, at least a token investigation beyond the information provided by the IDS is required to determine whether the event is a false positive or warrants further attention. The easier it is for an analyst to make this decision, the more efficient the entire system becomes. EnCase Enterprise is capable of providing the information an analyst needs to make such a decision.

The three main mechanisms for sorting out the unknown information are Filters, EnScripts and Conditions. Guidance provides defaults for each of these, but the user can add more.

We found EnCase Enterprise filters to be very basic, handling file permissions, deleted files and specific types of Web pages.

EnScript is a proprietary language that lets you build code for complex activities, such as collecting data from the Servlet, initializing databases and setting up filter combinations. The name of the EnScript that polls data from the Servlet is Enterprise Sweep. By default, it captures only port, file, process and physical system information. However, the user is presented with approximately 25 optional modules for data collection that can be selected. For example, in our tests we retrieved log files for Windows and Linux via

How we did it

The SAFE was installed on a dual-Xeon Dell Precision with 1G byte RAM running Windows 2003 Server Enterprise. The Examiner was installed on a Pentium IV Dell Dimension with 1G byte RAM running Windows XP Professional. The target machines examined were a mix of Windows 2000 Server, Windows XP Professional, RedHat 9.0 and RedHat Fedora Core 3. All systems were connected via Linksys 10/100M bit/sec hub. Different aspects of the incident response functionality of EnCase Enterprise were exercised after installing both rootkits (Hacker Defender and FU) and command and control (Optix) programs. As the greater functionality of EnCase Enterprise focuses on Windows for detecting these types of tools, the majority of testing was done with Windows targets.

Announcing...
IT Roadmap: Conference & Expo

Featured IT Track: Application and Content Security

An all-NEW free event from Network World!

1 day. 6 tracks. 40+ IT all-stars, analysts, case-studies and vendor solutions.

COMING TO: BOSTON, CHICAGO, DALLAS & BAY AREA

Register today!

Case 1:04-cr-10217-GAO Document 75-3 Filed 03/03/2006 Page 5 of 7

the Windows Event Log Parser and Linux SysLog Parser, respectively.
Continued

1 | 2 | Next >>

print send to a friend feedback reprint

Print Subscription

Related Article >

VENDOR SOLUTIONS

White Papers

Want to Simplify Identity Management?
- Quest Software

E-Policy Best Practices Guide
- St. Bernard

"The Definitive Guide to Active Directory Disaster Recovery"
- NetPro Computing Inc

More...

Special Report

Secure Enterprise Wireless: Today's Management Challenges - Siemens
For a century, over-the-air transmission has been so fundamental to the evolution of technology that today's world would be impossible without it. Yet it has only been recently that wireless has been successfully introduced as a convenient and reliable local-area network (LAN) technology in the enterprise. Why the long wait? The answer can largely be reduced to two words: reliability and security. This special report examines some of the issues that confront todayÃ½s enterprise as it meets the wireless challenge. Click here to download now,

SPONSORED LINKS

Buy a link

Free Tech Day Seminar
Learn from Symantec Experts how to Protect Your Network. Enroll Today!

Security Within - Configuration based Security
Configuration and policy based security systems are a pro-active way to defend against IT security attacks. Click here to request our white papers, "Security Within - Configuration based Security" and "Policy Management vs. Vulnerability Scanning".

System Management for new Enterprise environments
Request white paper which outlines the case for an IT Portal architecture to meet the new requirements placed on IT management. These requirements include IT security; SOX, HIPAA, FISMA compliance; managing outsourcing contracts; and more.

Authentication TCO White Paper from VeriSign
Discover how to secure multiple devices across your enterprise, plus reduce TCO and complexity by implementing a two-factor unified authentication solution. Leverage your existing infrastructure. Learn more.

Case 1:04-cr-10217-GAO Document 75-3 Filed 03/03/2006 Page 6 of 7

Secure Sockets Layer (SSL) Certificates secure ecommerce transactions.- **Verisign**

Build operational efficieny into your enterprise.- **Microsoft Corp**

Does Your Infrastructure Deliver? Web Application Acceleration can help.- **Akamai**

Want a VoIP solution without jitter, latency and packet loss? Get Juniper Networks VoIP.- **Juniper Networks**

Download a FREE trial of Trend Micro Enterprise Anti-Spyware Solutions.- **TREND MICRO**

Explore Tested Encryption Products - Download this free Executive Guide: Ensuring E-mail Security - **MessageLabs**

Network World Special Report: Securing Wireless Enterprises, Today's Management Challenge , click here to download - **Siemens**

Learn how to drive efficiency while maintaining security in a mobile enterprise.- **Avaya**

Pillar Axiom reduces complexity and costs with both SAN & NAS on one system- **Pillar Data Systems, Inc.**

New Webcast! The Seven Deadly Sins of Deploying Wireless: ProCurve and AirWave Deliver a Comprehensive Solution- **ProCurve Networking by HP**

Microsoft Free Security Tools & Updates- **Microsoft Corp**

Microsoft SQL Server 2005. Learn More.- **Microsoft Corp**

Microsoft Windows Server delivers a lower TCO.- **Microsoft Corp**

Tune in to hear how Mirapoint simplified email at the George Washington School of Law.- **Mirapoint**

Five Strategies for Deploying Blades into Existing Data Centers. View this exclusive webcast now:- **APC**

Hear ShoreTel customers discuss the challenges of migrating from TDM PBX to IP telepho- **Shoretel**

FREE SUBSCRIPTION TO NETWORK WORLD

Receive the latest Network IT news and information!
Sign up today for 50 FREE weekly issues of Network World.

First Name Last Name

E-mail Zip Code

Research Centers: Applications | Application Development | Applications-Standards | Applications Vendor Solutions | Collaboration | CRM / ERP | Databases | Directories | Grid Computing | Java | Messaging | .Net | RFID | SOAP | Web Services | XML | **Convergence & VoIP** | Convergence Regulatory | Convergence Services | Convergence Standards | Convergence VoIP Vendor Solutions | Video | IP PBX | SIP | VoIP | VoIP Services | **E-Business** | DNS | RFID | Supply Chain | Web security **LANs & Routers** | Acceleration | Gigabit Ethernet | Lans-Standards | Routers | Wireless LANs | **Network Management** | Application Management | Desktop Management | Management Test Patch Management | **Operating Systems** | Linux | NetWare | Unix | Windows **Outsourcing** | Managed Services | Offshoring **Security** | Firewalls - VPN - Intrusion | Identity management | Patch Management | Microsoft Security | Privacy | Security Standards | Spam & Phishing | Viruses & worms | Web Security | Wireless Security | **Servers & Desktop** | Backup-Recovery | DataCenter | Desktops | Desktop Management | Grid | Servers | Server Blades | Servers Desktops | Utility Computing | **Small & Medium Business** | Broadband | Telework | Handhelds & PDAs | Home Networking | Security | **Storage** | Compliance | Infiniband | Network-Attached Storage | SANs | Storage

Case 1:04-cr-10217-GAO Document 75-3 Filed 03/03/2006 Page 7 of 7

Management | Storage Virtualization | Virtualization | **Vendor News** | Bankruptcy | Earnings | Lawsuits | Layoffs | Standards | Start Ups | **Vendor Markets** | Education | Financial | Healthcare | HIPAA | Manufacturing | Retail | **Wide Area Network** | Broadband | Carriers | Frame Relay | Metro Ethernet | MPLS | Service providers | Wireless services | **Wireless & Mobile** | Wireless LANs | PDAs & handhelds | Wireless Security | Wireless Services | Wireless Standards | Wireless Switches | **All Company Profiles**

Contact Us | Terms of Service/Privacy | Media Guide | Reprints and links | Partnerships | Subscribe to NW | About Network World, Inc.

Copyright, 1994-2006 Network World, Inc. All rights reserved.

Web design by Network World in alliance with Ceonex Web Development

IDG Network: Bio-IT World CIO CMO Computerworld CSO Darwin Demo GamePro GameStar.com GamerHelp.com Infoworld IT Careers IT World Canada JavaWorld.com Macworld MacCentral.com Outsourcing World PC World Playlistmag.com